## Amendments to the Claims

Claims 1-18 **(Canceled)**

Claim 19 **(Currently Amended)** A playback terminal for playing back content, the playback terminal comprising:

a content read unit operable to read encrypted content from a portable medium, the encrypted content being generated by encrypting content using at least medium information pre-recorded on the portable medium and information pre-stored in the playback terminal;

a decryption method judgment unit operable to judge whether or not information managed by an external license server is required for decrypting the encrypted content;

a medium information read unit operable to read the medium information pre-recorded on the portable medium;

a communication unit operable to acquire the managed information managed by the external license server when it is judged that the managed information is required, the managed information managed by the external license server being a part of information which is required for the decryption of the encrypted content;

a medium content key calculation unit operable to cryptographically calculate a medium content key using the medium information and the information pre-stored in the playback terminal itself;

a license content key calculation unit operable to cryptographically calculate a license content key using the medium content key and the managed information acquired from the external license server; and

a decryption unit operable to (a) decrypt the encrypted content using ~~only~~ the medium ~~information~~ content key ~~and the information pre-stored in the playback terminal itself, without using the managed information managed by the external license server~~, when it is judged that the managed information is not required, and (b) decrypt the encrypted content using the license content key ~~managed information acquired from the external license server, the medium information and the information pre-stored in the playback terminal itself~~, when it is judged that the managed information is required.

Claim 20 **(Currently Amended)** The playback terminal of claim 38, wherein

the medium information includes a media key,

the medium content key calculation unit cryptographically calculates the medium content key using the media key of the medium information, and

the decryption unit includes:

a content key obtaining sub-unit operable to, when it is judged that the rights information is not required, ~~obtain the media key from the medium information and, using the obtained media key,~~ obtain ~~a first~~ the medium content key used in decrypting of the encrypted content; and

a content decryption sub-unit operable to, when it is judged that the rights information is not required, decrypt the encrypted content using the ~~first~~ medium content key.

Claim 21 **(Currently Amended)** The playback terminal of claim 20, wherein

the content key obtaining sub-unit, when it is judged that the rights information is required, obtains the license ~~a second~~ content key used in decrypting of the encrypted content, ~~using the rights information~~, and

the content decryption sub-unit, when it is judged that the rights information is required, decrypts the encrypted content using the license ~~second~~ content key.

Claim 22 **(Currently Amended)** The playback terminal of claim 21, wherein

the ~~The~~ rights information includes a rights key,

the license content key calculation unit cryptographically calculates the license content key using the rights key of the rights information, and

the content key obtaining sub-unit, when it is judged that the rights information is required, obtains the license ~~second~~ content key using the rights key.

Claim 23 **(Canceled)**

Claim 24 **(Previously Presented)** The playback terminal of claim 21, wherein

the portable medium further has stored thereon key obtaining information indicating whether or not the rights information is required for obtaining a key used for decrypting the encrypted content, and

the playback terminal further comprises:

a key obtaining information read unit operable to read the key obtaining information from the portable medium, wherein

the decryption method judgment unit performs the judgment of whether or not the rights information is required for decrypting the encrypted content, based on the key obtaining information.

Claim 25 **(Currently Amended)** The playback terminal of claim 20, wherein

the decryption unit, when it is judged that the rights information is necessary, performs decryption of the encrypted content only when the communication ~~rights information acquisition~~ unit has already acquired the rights information and the rights information indicates that usage of the content is permitted.

Claim 26 **(Currently Amended)** The playback terminal of claim 20, further comprising:

a holding unit operable to hold device unique information that is unique to the playback terminal, wherein

the media key is in an encrypted state, having been encrypted using the device unique information, and

the medium content key calculation unit ~~content key obtaining sub-unit~~, when it is judged that the rights information is not required, obtains the media key by decrypting the encrypted-state media key using the device unique information.

Claim 27 **(Previously Presented)** The playback terminal of claim 20, wherein

the portable medium further has stored thereon information indicating whether or not the rights information is required for decrypting of the encrypted content, and

the playback terminal further comprises:

an information read unit operable to read the information from the portable medium, wherein

the decryption method judgment unit performs the judgment of whether or not the rights information is required for decrypting the encrypted content, based on the information.

Claim 28 **(Currently Amended)** A content playback method used in a playback terminal for playing back content, the content playback method comprising:

reading encrypted content from a portable medium, the encrypted content being generated by encrypting content using at least medium information pre-recorded on the portable medium and information pre-stored in the playback terminal;

judging whether or not information managed by an external license server is required for decrypting the encrypted content;

reading the medium information pre-recorded on the portable medium;

acquiring the managed information managed by the external license server when it is judged that the managed information is required, the managed information managed by the external license server being a part of information which is required for the decryption of the encrypted content;

cryptographically calculating a medium content key using the medium information and the information pre-stored in the playback terminal itself;

cryptographically calculating a license content key using the medium content key and the managed information acquired from the external license server; and

a decryption step of (a) decrypting the encrypted content using ~~only~~ the medium ~~information~~ content key ~~and the information pre-stored in the playback terminal itself, without using the managed information managed by the external license server~~, when it is judged that the managed information is not required, and (b) decrypting the encrypted content using the license content key ~~managed information acquired from the external license server, the medium information and the information pre-stored in the playback terminal itself~~, when it is judged that the managed information is required.

Claim 29 **(Currently Amended)** The content playback method of claim 41, wherein

the medium information includes a media key,

the cryptographically calculating of the medium content key comprises cryptographically calculating the medium content key using the media key of the medium information, and

the decryption step includes:

a content key obtaining sub-step of, when it is judged that the rights information is not required, ~~obtaining the media key from the medium information and, using the obtained media key,~~ obtaining the medium ~~a first~~ content key used in decrypting of the encrypted content; and

a content decryption sub-step of, when it is judged that the rights information is not required, decrypting the encrypted content using the medium ~~first~~ content key.

Claim 30 **(Currently Amended)** The content playback method claim 29, wherein

the content key obtaining sub-step includes, when it is judged that the rights information is required, obtaining the license ~~a second~~ content key used in decrypting of the encrypted content, ~~using the rights information,~~ and

the content decryption sub-step includes, when it is judged that the rights information is required, decrypting the encrypted content using the ~~second~~ license content key.

Claim 31 **(Currently Amended)** The content playback method of claim 30, wherein

the rights information includes a rights key,

the cryptographically calculating of the license content key comprises cryptographically calculating the license content key using the rights key of the rights information, and

the content key obtaining sub-step includes, when it is judged that the rights information is required, obtaining the ~~second~~ license content key using the rights key.

Claim 32 **(Canceled)**

Claim 33 **(Previously Presented)** The content playback method of claim 30, wherein

the portable medium further has stored thereon key obtaining information indicating whether or not the rights information is required for obtaining a key used for decrypting the encrypted content, and

the content playback method further comprises:

reading the key obtaining information from the portable medium, wherein

the judging comprises judging whether or not the rights information is required for decrypting the encrypted content, based on the key obtaining information.

Claim 34 **(Previously Presented)** The content playback method of claim 29, wherein

the decryption step includes, when it is judged that the rights information is necessary, performing decryption of the encrypted content only when the acquiring has already acquired the rights information and the rights information indicates that usage of the content is permitted.

Claim 35 **(Currently Amended)** The content playback method of claim 29, wherein

the playback terminal includes a holding unit operable to hold device unique information that is unique to the playback terminal,

the media key is in an encrypted state, having been encrypted using the device unique information, and

the cryptographically calculating of the medium content key ~~content key obtaining sub-step~~ includes, when it is judged that the rights information is not required, obtaining the media key by decrypting the encrypted-state media key using the device unique information.

Claim 36 **(Previously Presented)** The content playback method of claim 29, wherein

the portable medium further has stored thereon information indicating whether or not the rights information is required for decrypting of the encrypted content, and the content playback method further comprises:

reading the information from the portable medium, wherein

the judging comprises judging whether or not the rights information is required for decrypting the encrypted content, based on the information.

Claim 37 **(Currently Amended)** A portable recording medium having storing thereon

medium information,

encrypted content, and

indicating information indicating whether or not rights information managed by an external license server is required for decrypting the encrypted content, wherein

the encrypted content is data generated by encrypting content using at least the medium information and information pre-stored in a playback terminal, so that (a) a medium content key cryptographically calculated using the medium information and the information pre-stored in the playback terminal, without using the rights information, ~~are~~ is required for decrypting the encrypted content, when the indicating information indicates that the rights information is not required, and (b) a license content key cryptographically calculated using the medium content key ~~the medium information, the information pre-stored in the playback terminal,~~ and the rights information ~~are~~ is required for decrypting the encrypted content, when the indicating information indicates that the rights information is required.

Claim 38 **(Currently Amended)** The playback terminal of claim 19, wherein

the ~~The~~ managed information managed by the external license server is rights information including usage rights for the content,

the decryption method judgment unit judges whether or not the rights information is required for decrypting the encrypted content,

the communication unit acquires the rights information from the external license server when it is judged that the rights information is required,

the license content key calculation unit calculates the license content key using the medium content key and the rights information acquired from the external license server, and

the decryption unit (a) decrypts the encrypted content using the medium content key ~~only the medium information and the information pre-stored in the playback terminal itself, without using the rights information~~, when it is judged that the rights information is not required, and (b) decrypts the encrypted content using the license content key ~~rights information, medium information and the information pre-stored in the playback terminal itself~~, when it is judged that the rights information is required.

Claim 39 **(Previously Presented)** The playback terminal of claim 20, wherein

the rights information includes information showing permission to play back the content.

Claim 40 **(Previously Presented)** The playback terminal of claim 39, wherein

the portable medium further has recorded thereon information indicating whether or not the rights information is necessary for decrypting the encrypted content, and

the decryption method judgment unit judges whether or not the rights information is required for decrypting the encrypted content based on the information recorded on the portable medium.

Claim 41 **(Currently Amended)** The content playback method of claim 28, wherein

the ~~The~~ managed information managed by the external license server is rights information including usage rights for the content,

the judging comprises judging whether or not the rights information is required, as the information managed by the external license server, for decrypting the encrypted content,

the acquiring comprises acquiring the rights information from the external license server when it is judged that the rights information is required, and

the decryption step comprises (a) decrypting the encrypted content using ~~only~~ the medium content key ~~information and the information pre-stored in the playback terminal itself, without using the rights information~~, when it is judged that the rights information is not required, and (b) decrypting the encrypted content using the license content key ~~rights information, medium information and the information pre-stored in the playback terminal itself~~, when it is judged that the rights information is required.

Claim 42 **(Previously Presented)** The playback terminal of claim 26, wherein

the encrypted-state media key recorded on the recording medium is generated by encrypting the media key using device information of valid playback terminals, and

the content key obtaining unit fails to obtain the media key by decrypting the encrypted-state media key, when the device information of the playback terminal itself is not included in the device information of the valid playback terminals.